NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Oil well blowout reported near Lake Sakakawea. A roaring out-of-control oil well spewed an orange-colored mix of gas, oil, and saltwater as high as 50 feet into the air December 13 near Lake Sakakawea in North Dakota, staining the snowy white ground as far as 1,000 feet from the well in the prevailing wind direction. A backhoe bucket was finally lowered over the wellhead, capping the spew, and forcing all the escaping liquids to remain inside a containment berm around the well. The Slawson Exploration well is about 10 miles southwest of Parshall, near the Van Hook Arm recreation site. A Slawson superintendent said the bucket was pulled back off the well later because of fire and safety concerns. Crews prepped the location and were prepared to go in December 14 to get the well under control, he said. Officials also received reports December 13 of a spill from an oil well near Johnson's Corner east of Watford City. That well was shut in within a few hours. The superintendent said he did not yet know what failed during the workover operation. He said the well had been in production for about a month and is among 20 Slawson wells in the immediate area and 300 in North Dakota. He said if the well is controlled by December 14, as expected, the workover operation could resume. A State-owned wildlife management area borders the field where the well is located. The saltwater that came up with the oil was the most toxic. A North Dakota Health Department environmental engineer said well records will detail out how much oil, gas, and saltwater spilled during the blowout. Source: http://bismarcktribune.com/bakken/oilwellblowoutreportednearlakesakakawea/article_faee38bc-4548-11e2-869c-0019bb2963f4.html

Regional

Nothing Significant to Report

National

Nothing Significant to Report

International

Nothing Significant to Report

Banking and Finance Industry

New findings lend credence to Project Blitzkrieg. "Project Blitzkrieg," a brazen Underweb plan for hiring 100 botmasters to fuel a blaze of ebanking heists against 30 U.S. financial institutions in the Spring of 2013, was met with skepticism from some in the security community after news of the scheme came to light in October. But new research suggests the crooks who hatched the plan were serious and have painstakingly built up a formidable crime machine in preparation for the project. Krebs on Security reported December 12. McAfee said it tracked hundreds of infections from the Gozi Prinimalka trojan since Project Blitzkrieg was announced in early

September. vorVzakone, the miscreant who posted the call-to-arms, also posted a number of screen shots that he said were taken from a working control panel for the botnet he was building. According to RSA Security, the botnet consisted of systems infected with Gozi Prinimalka, a closely-held, custom version of the powerful password-stealing Gozi banking trojan. In an analysis to be published December 13, McAfee said it was able to combine the data in those screen shots with malware detections on its own network to correlate both victim PCs and the location of the control server. It found that the version of the Prinimalka trojan used in the attack has two unique identifiers that identify what variant is being deployed on infected computers. McAfee said that all of the systems it identified from the screen shots posted by vorVzakone carried the Campaign ID 064004, which was discovered in the wild on April 14. A threat researcher at McAfee said the company's analysis indicates that Project Blitzkrieg is a credible threat to the financial industry and appears to be moving forward. The researcher posits that vorVzakone most likely intended to hire botmasters who already had access to substantial numbers of login credentials for the U.S. financial institutions targeted in the scheme. Several banks were indicated on a target list, including Bank of America, Capital One, and Suntrust, but many of the targets are in fact investment banks, such as American Funds, Ameritrade, eTrade, Fidelity, OptionsExpress, and Schwab. Source: http://krebsonsecurity.com/2012/12/new-findings-lend-credence-to-project-blitzkrieg/

4 banks respond to DDoS threats. The day after a hacktivist group announced plans to launch a second wave of distributed-denial-of-service (DDoS) attacks on five U.S. banks, SunTrust suffered intermittent outages and Bank of America and PNC said small numbers of their customers reported having trouble accessing their sites, BankInfoSecurity reported December 12. But it remained unclear whether the problems were the result of an attack. PNC used social media to warn consumers that site outages should be expected, but that account and online-banking credentials would remain secure. The onlinemonitoring site websitedown.com reported that the SunTrust Banks Web site suffered intermittent outages. A Bank of America (BofA) spokesman said that while BofA's site suffered no overall outages, an isolated number of online-banking users reported problems accessing the site. A PNC spokeswoman said some PNC customers may have experienced intermittent difficulty logging in on their first attempts. And a U.S. Bank spokesman said that the bank is "taking all necessary steps" to prepare for more attacks. Source: http://www.bankinfosecurity.com/4-banks-respond-to-ddos-threats-a-5350/op-1

HSBC to pay $1.9 billion U.S. fine in moneylaundering case. HSBC has agreed to pay a record $1.92 billion fine to settle a multiyear probe by U.S. prosecutors, who accused Europe's biggest bank of failing to enforce rules designed to prevent the laundering of criminal cash, Reuters reported December 11. The U.S. Department of Justice (DOJ) charged the bank with failing to maintain an effective program against money laundering and conduct due diligence on certain accounts. It also charged the bank with violating sanctions laws by doing business with customers in Iran, Libya, Sudan, Burma, and Cuba. In an agreement with the DOJ, the bank will take steps to fix the problems, pay a fine of $1.256 billion, and retain a compliance monitor to resolve the charges through a deferred-prosecution agreement. Including penalties imposed by other agencies, the bank's fines totaled $1.92 billion. HSBC also faces civil penalties, to be

announced later December 11. The settlement offers new information about failures at HSBC to police transactions linked to Mexico, details of which were reported this summer in a U.S. Senate probe. Between 2006 and 2010, HSBC ignored money-laundering risks associated with certain Mexican customers and allowed at least $881 million in drug trafficking proceeds, including proceeds from the Sinaloa Cartel in Mexico and the Norte del Valle Cartel in Colombia, to be laundered through the bank, according to the agreement. HSBC said it expected to also reach a settlement with British watchdog the Financial Services Authority.
Source: http://www.reuters.com/article/2012/12/11/us-hsbc-probeidUSBRE8BA05M20121211

Skimming, trapping threatened ATMs in 2012: Survey. Fraud and physical attacks against ATMs rose globally in 2012, according to a survey of 225 respondents worldwide released December 6 by the ATM Industry Association. According to the survey, the swiping of details embedded in the magnetic stripes of debit and credit cards inserted into ATMs remains the top threat to ATM security, followed by the deployment of devices that trap cash or cards and prevent them from being dispensed to customers. The use of gas and explosives to destroy ATMs increased in the past six months as well, according to the survey. Forty-five percent of those surveyed said criminal attacks on ATMs in their country or region rose since the second quarter, while 53 percent said fraud and attacks on ATMs have added costs to their businesses. Roughly 54 percent of respondents said they invested more in security technology compared with six months ago, while 42 percent report no change in their investment. Source: http://www.americanbanker.com/issues/177_235/skimming-trapping-threatened-atms-in-2012-survey-1055023-1.html

Chemical and Hazardous Materials Sector

OSHA releases online tool to help protect workers exposed to cadmium. The Occupational Safety and Health Administration (OSHA) December 11 released a new interactive online tool to help protect workers exposed to cadmium. The new interactive online tool will assist employers in complying with OSHA's cadmium standard. OSHA's Cadmium Biological Monitoring Advisor analyzes biological monitoring results provided by the user. These data, along with a series of answers to questions generated by the cadmium advisor, are used to determine the biological monitoring and medical surveillance requirements that must be met under the general industry cadmium standard. These requirements include the frequency of additional monitoring and other mandatory components of the employer's medical surveillance program. The cadmium advisor is primarily intended for use by experienced medical professionals who assess workers' cadmium exposure. It may also be useful as an educational tool for workers and members of the general public by providing information on what constitutes overexposure to cadmium and what to do to prevent exposure on the job. Source: http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=23391

Commercial Facilities

(Connecticut) **At least 26 dead in shooting at Connecticut elementary school.** Twenty-seven people, including 20 children, were killed December 14 when a gunman opened fire inside his mother's kindergarten class at a Newtown, Connecticut elementary school. The shooter gunned down his mother and her entire class at Sandy Hook Elementary School; at the time of this report none of the pupils in the classroom were accounted for, according to local news sources. The gunman was found dead inside the school, according to officials. A source told Fox News that the shooter's father, who was divorced from his ex-wife, was killed at his home in New Jersey. Police were also searching for two friends of the killer, who were unaccounted for at the time of this report. The shooter's girlfriend and another friend were missing in New Jersey, according to law enforcement sources. An official with knowledge of the situation said the shooter was armed with a .223-caliber rifle. Four weapons in total were recovered from the scene. The motive was not yet known. The elementary school has close to 700 students. Source: http://www.foxnews.com/us/2012/12/14/police-respond-to-shooting-atconnecticut-elementary-school/

(Oregon) **Police say Oregon mall shooter used stolen rifle in attack.** The gunman who killed two people and himself in a shooting rampage at a Portland, Oregon mall used a stolen rifle from someone he knew, authorities said December 12. The gunman armed himself with an AR-15 semiautomatic rifle and had several fully loaded magazines when he arrived at a the mall December 11, said the Clackamas County sheriff. The sheriff said the rifle jammed during the attack, but he managed to get the weapon working again. The gunman wore a hockey-style face mask, parked his personal vehicle in front of the second-floor entrance to Macy's, and walked briskly through the store, into the mall, and began firing randomly, police said. He then fled along a mall corridor and into a back hallway, down stairs, and into a corner where police found him dead from an apparent self-inflicted gunshot. Source: http://www.pasadenastarnews.com/news/ci_22179373/police-say-oregon-mall-shooter-used-stolen-rifle

Communications Sector

Yet another eavesdrop vulnerability in Cisco phones. A university student presenting at the Amphion Forum demonstrated turning a Cisco VoIP phone into a listening device, even when it is on the hook, The Register reported December 13. The vulnerability demands a fairly extensive reconfiguration of the phone, according to Dark Reading. This, at least, means the attacker needs greater sophistication than previous eavesdropper attacks reported by The Register in 2007 and 2011. A number of 7900-series phones are affected, according to Forbes. The latest vulnerability is based on a lack of input validation at the syscall interface, according to Columbia University graduate student. He said this "allows arbitrary modification of kernel memory from userland, as well as arbitrary code execution within the kernel. This, in turn, allows the attacker to become root, gain control over the DSP [Digital Signal Processor], buttons, and LEDs on the phone." In the demonstration, the student modified the DSP to surreptitiously turn on the phone's microphone and stream its output to the network. To

simplify the demonstration, he programmed the necessary reconfiguration onto an external circuit which he plugged into the phone's Ethernet port, and then captured what was spoken near the VoIP phone on his smartphone. The student told Dark Reading that the phones contain a number of vulnerable third-party libraries, which he promises to discuss at the upcoming Chaos Computer Conference, 29C3. Cisco said workarounds and a software patch are available to address the issue, tagged with the bug id CSCuc83860. Source: http://www.theregister.co.uk/2012/12/13/cisco_voip_phones_vulnerable/

GPS software attacks more dangerous than jamming and spoofing, experts say. Security researchers from Carnegie Mellon University, in collaboration with experts from Coherent Navigation, identified new attack vectors against the Global Positioning System (GPS), Softpedia reported December 10. According to the researchers, a malicious 45-second GPS broadcast is capable of taking down more than 30 percent of the Continually Operating Reference Station (CORS) network, which is used for safety and life-critical applications. Furthermore, it could also disrupt 20 percent of the Networked Transport of RTCM via Internet Protocol (NTRIP) systems. A total of three new attack methods have been identified: GPS data level attacks, GPS receiver software attacks, and GPS dependent system attacks. GPS data level attacks are somewhat similar to spoofing, but they can cause more damage. For instance, such an attack can remotely crash a high-end receiver. The second type of attacks leverages the fact that GPS receivers run some kind of computer software that can be remotely compromised. Since GPS receivers are most often seen as devices instead of computers, the security holes leveraged by attackers can remain unpatched for extended periods of time. In order to mitigate such threats, experts recommend stronger verification of GPS receiver software and the deployment of regular software updates for IP-enabled devices. Another mitigation strategy refers to the use of Electronic GPS Attack Detection System (EGADS) that alerts users when an attack is underway, and an Electronic GPS Whitening System (EGWS) that re-broadcasts a whitened signal to otherwise vulnerable receivers. One noteworthy thing about these types of attacks is that they do not require sophisticated or expensive equipment. The hardware utilized by the researchers costs only about $2,500. Source: http://news.softpedia.com/news/GPS-Software-Attacks-More-Dangerous-Than-Jamming-and-Spoofing-Experts-Say-313388.shtml

CRITICAL MANUFACTURING

NHTSA recall notice - Acura MDX and Honda Odyssey and Pilot interlock levers. Honda announced December 13 the recall of 807,161 model year 2003 and 2004 Pilot and Odyssey and 2003 through 2006 Acura MDX passenger vehicles manufactured from November 26, 2001 through August 30, 2006. The interlock lever of the ignition switch may deform, which can allow the interlock function of a vehicle with an automatic transmission to be defeated. Removal of the ignition key when the gear selector of a vehicle with an automatic transmission has not been shifted to the park position can allow the vehicle to roll away, increasing the risk of a crash. Honda will notify owners and instruct them to take their vehicle to a Honda or Acura dealer. The dealer will install an updated shift interlock lever and, if necessary, replace the ignition switch. Source: http://www-

odi.nhtsa.dot.gov/recalls/recallresults.cfm?start=1&SearchType=QuickSearch&rcl_ID=12V573000&summary=true&prod_id=203623&PrintVersion=YES

Defense/ Industry Base Sector

Nothing Significant to Report

Emergency Services

U.S. law enforcement busts cybercrime rings with help from Facebook. U.S. law enforcement agencies with the help of Facebook arrested 10 persons from various countries in connection with international cybercrime rings that targeted users on the social network. The operation is said to have identified international cybercrime rings that used various variants of a malware called Yahos. The malware infected more than 11 million computers and caused over $850 million in losses through a Butterfly botnet, which steals computer users' credit card, bank account, and other personal identifiable information, the FBI said in a statement. The 10 persons arrested are from Bosnia and Herzegovina, Croatia, Macedonia, New Zealand, Peru, the U.K., and the U.S. Facebook's security team assisted the law enforcement agencies in the investigation by helping "to identify the root cause, the perpetrators, and those affected by the malware," the FBI said. Yahos targeted Facebook users from 2010 to October this year, and security systems were able to detect affected accounts and provide tools to remove these threats, the FBI said. Source: http://www.itworld.com/security/327524/us-law-enforcement-bustscybercrime-rings-help-facebook

Energy

Hackers breached heating system via industrial control system backdoor. Hackers broke into the industrial control system (ICS) of a New Jersey air conditioning company earlier this year, using a backdoor vulnerability in the system, according to a FBI memo made public the week of December 10. The intruders first breached the company's ICS network through a backdoor in its Niagara AX ICS system, made by Tridium. This gave them access to the mechanism controlling the company's own heating and air conditioning, according to a memo prepared by the FBI's office in Newark. The breach occurred in February and March, several weeks after someone using the Twitter moniker @ntisec posted a message online indicating that hackers were targeting supervisory control a and data acquisition (SCADA) systems, and that something had to be done to address vulnerabilities. The individual had used the Shodan search engine to locate Tridium Niagara systems that were connected to the internet and posted a list of URLs for the systems online. One of the IP addresses posted led to the New Jersey company's heating and air conditioning control system. The company used the Niagara system notonly for its own HVAC system, but also installed it for customers, which included banking institutions and other commercial entities, the memo noted. An IT contractor who worked for the company told the FBI that the company had installed its own control system directly connected to the internet with no firewall in place to protect it. Although the system was password protected in general, the backdoor through the IP address apparently required no password and allowed direct

access to the control system. The backdoor URL gave access to a Graphical User Interface (GUI), "which provided a floor plan layout of the office, with control fields and feedback for each office and shop area," according to the FBI. "All areas of the office were clearly labeled with employee names or area names." Forensic logs showed that intruders had gained access to the system from multiple IP addresses in and outside the U.S. Source: http://www.wired.com/threatlevel/2012/12/hackers-breach-ics/

Food and Agriculture

Japan halts beef imports from Brazil on BSE fears. Japan has stopped importing beef from Brazil after the World Animal Health Organization (OIE) discovered a protein believed to cause bovine spongiform encephalopathy (BSE) in a cow, Meat & Poultry reported December 10. OIE conducted tests on tissue from the Brazilian cow and confirmed the presence of prions, the protein linked to BSE. The OIE report stated that the animal was a beef breeding cow almost 13 years old when it died, according to information obtained during the epidemiological investigations. "The epidemiological investigation shows that the animal's death was not caused by BSE and suggests that it may be an atypical case of the disease occurring in the oldest animals," OIE said in its findings. "Information collected during the epidemiological investigation shows also that the animal was reared in an extensive system on grazing." OIE added that Brazil is still recognized as having a negligible BSE risk. Source: http://www.meatpoultry.com/News/NewsHome/Global/2012/12/JapanhaltsbeefimportsfromBrazil on BSE fears.aspx

Consumers, industry benefit under FSIS hold and test implementation. The U.S. Department of Agriculture's (USDA) Food Safety and Inspection Service (FSIS) December 7 announced that, beginning in 60 days, the Agency will require producers to hold shipments of non-intact raw beef and all ready-to-eat products containing meat and poultry until they pass testing for foodborne adulterants. The new policy requires official establishments and importers of record to maintain control of products tested for adulterants by FSIS and not allow the products to enter commerce until negative test results are received. FSIS anticipates most negative test results will be determined within two days. The policy applies to non-intact raw beef products or intact raw beef products intended for non-intact use and that are tested by FSIS for Shiga-toxin producing Escherichia coli. Also, the policy applies to any ready-to-eat products tested by FSIS for pathogens. Source: http://www.fsis.usda.gov/News_&_Events/NR_120712_01/index.asp

Government Sector (including Schools and Universities)

(California) **State of Calif. mistakenly publishes thousands of SSN online.** Officials confirmed that the State of California mistakenly published thousands of Social Security numbers on the Internet, KCRA reported December 11. The confidential information was available on the State's Medi-Cal Web site for anyone to see for a period of 9 days, before the mistake was

discovered and the numbers removed. The list includes Medi-Cal providers in 25 California counties. State officials from the Department of Health Care Services admitted in an interview to the posting of nearly 14,000 Social Security numbers belonging to Medi-Cal providers working for In-Home Supportive Services. "This was inadvertent and we sincerelyregret this has happened," said the deputy director for public affairs for the Department of Health Care Services. Source: http://www.kcra.com/news/StateofCalifmistakenlypublishesthousandsofSSNonline//11797728/17723434/-/tad6swz/-/index.html?absolute=true

(Mississippi) **Bomb threats called in to 29 county courthouses in Mississippi.** Twenty-nine county courthouses throughout Mississippi received bomb threats December 12. Officials in the coastal counties said all south Mississippi courthouses have been cleared for re-admittance December 13. The executive director of the Mississippi office of the Department of Homeland Security said 31 total threats were received in 29 counties. The threats were similar to those received in November in Nebraska, Oregon, Tennessee, and Washington. None of those threats were credible. Officials said the calls came in to the circuit clerk's offices. A George County official described the voice as sounding recorded and said the caller's number was blocked. The executive director said Homeland Security is looking for the person responsible for the calls. Source: http://www.sunherald.com/2012/12/12/4355810/bomb-threats-called-in-to-29-county.html

Information Technology and Telecommunications

Only 15% of known malware caught by Android 4.2's verifier. A researcher at North Carolina State University found that only 15 percent of known malware samples tested on Android 4.2's new app verification service were detected. The researcher loaded 1260 malware samples from the Android Malware Genome Project onto 10 Android 4.2 devices. Of the 1260 samples only 193 were detected as malware. The researcher also performed a test comparing Google's verification against a range of ten different existing anti-virus applications through VirusTotal, looking at randomly selected malware samples from each malware family. The anti-virus applications run by VirusTotal ranged in efficacy from 100 percent to 51 percent, but the Android App verification system scored only 20.4 percent. The researcher noted that the app verification service uses a fragile mechanism of verifying SHA1 values from the app and package name to determine whether a package is dangerous or potentially dangerous. He also notes that the verification system relies on the server component, leaving the client-side of the system completely without detection capabilities. Source: http://www.honline.com/security/news/item/Only-15-of-known-malwarecaught-by-Android42sverifier-1765724.html

Fraudsters are setting up bogus hotel websites, experts find. Experts from security firm Bitdefender inform that fraudulent hotel Web sites can help criminals in accomplishing various malicious tasks, including identity theft and money laundering, Softpedia reported December 10. In other cases, they might simply ask individuals who want to book a room to pay a certain amount of money upfront. The fake Web sites usually leverage the names and reputations of

famous brands. Unlike phishing sites, these fraud Web sites are not promoted via email or social media spam. Instead, they are kept secret to ensure that the domain will not be seized by authorities. Source: http://news.softpedia.com/news/FraudsterAreSettingUpBogusHotelWebsites-Experts-Find-313528.shtml

(Texas) **Anonymous affiliate indicted for threats, stolen credit cards.** A federal grand jury in Dallas indicted a putative spokesman for the hacker collective known as Anonymous in connection with a massive data breach of Stratfor Global Intelligence. The man is in federal prison based on another indictment returned against him October 3. In that case he was charged with making a threat on the Internet, conspiring to make public restricted personal information of a federal employee, and retaliation against a federal law enforcement officer. One of the crimes he is accused of in the indictment is transferring a hyperlink from an Internet Relay Chat (IRC) channel apparently occupied by Anonymous to a channel controlled by himself. The hyperlink provided access to data stolen from Stratfor, which included more than 5000 credit card account numbers, information about their owners, and their Card Verification Values (CVV). By transferring and posting the hyperlink to the Internet, the man caused the data to be made available to persons online without the knowledge and authorization of Stratfor or the cardholders. He is also charged with possession of at least 15 credit card numbers and their CVV codes without the knowledge of the cardholders with intent to defraud them. In addition, the indictment accuses him of aggravated identity theft by knowingly transferring and possessing without lawful authority the means of identification of the credit card holders. Source: http://www.pcworld.com/article/2019242/anonymous-affiliate-indicted-for-threats-stolen-credit-cards.html

National Monuments and Icons

Nothing Significant to Report

Postal and Shipping

Nothing Significant to Report

Public Health

Nothing Significant to Report

Transportation

Nothing Significant to Report

Water and Dams

(Colorado) **Drilling spills reaching Colorado groundwater; State mulls test rules.** Oil and gas contaminated groundwater in 17 percent of the 2,078 spills and slow releases that companies reported to Colorado regulators over the past 5 years, State data showed. The damage was worse in Weld County, where 40 percent of spills reach groundwater, the Denver Post reported December 9. Most of the spills happened less than 30 feet underground — not in the deep well bores that carry drilling fluids into rock. State regulators said oil and gas crews typically worked on storage tanks or pipelines when they discover that petroleum material, which can contain cancer-causing benzene, has seeped into soil and reached groundwater. Companies respond with vacuum trucks or by excavating tainted soil. Contamination of groundwater — along with air emissions, truck traffic, and changed landscapes — has spurred public concerns about drilling along Colorado's Front Range. There are 49,236 active wells State-wide, up 31 percent since 2008, with 17,844 in Weld County. Colorado Oil and Gas Conservation Commission (COGCC) regulators that struggled to maintain a consistent set of State rules governing the industry would discuss with the groundwater issue December 10. The COGCC considered proposed changes to State rules that would require companies to conduct before-and-after testing of groundwater around wells to provide baseline data that could be used to hold companies accountable for pollution. Source: http://www.denverpost.com/environment/ci_22154751/drilling-spills-reaching-colorado-groundwater-state-mulls-test

Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168